解答例

STEP I 2016、第 7 問

純粋数学 • 4 を法とする因数分解

> **STEP I 2016、問 7**
>
> 先に進む前に、まず問題を読んでおこう。問題は STEP Support Programme の問題データベースにある：
>
> step.maths.org/questions/16-s1-q7

この問題は、*Beyond STEP* の第 1.7 節「**因数分解が破綻するとき**」で詳しく解説されている：https://beyondstep.keithmcnulty.org/ja/ch01/factorisation-fails.html

鍵となる考え方

すべては 4 を法として（modulo）考えることから導かれる。奇数は $\equiv 1$ または $\equiv 3 \equiv -1 \pmod 4$ であるから、奇数の積が S に属するか T に属するかは、T からの因数が偶数個か奇数個かによって決まる。この一つの偶奇（parity）の規則だけで、小問 (ii)、(iii)、(iv)(a) が解ける。小問 (iv)(b) では、S-素数が素数であるとは限らないこと、そしてそのために素因数分解の一意性（unique factorisation）が失われることに気づく必要がある。

解答

小問 (i)

正の奇数はすべて 4 で割った余りが 1 または 3 であり、偶数はそのどちらにもならない。よって $S \cup T$ は**正の奇数全体の集合**である。また、ある整数が異なる二つの余りをもつことはないので、$S \cap T$ は**空集合**（*empty set*）である。

小問 (ii)

$a, b \geq 0$ を整数として、S の元 $4a+1$ と $4b+1$ をとる。すると

$$(4a+1)(4b+1) = 16ab + 4a + 4b + 1 = 4(4ab + a + b) + 1,$$

であり、これは余りが 1 となる正の整数であるから、S に属する。

T については、答えは**否**である。たとえば $3 \in T$ であるが $3 \times 3 = 9 = 4 \times 2 + 1 \in S$ であり、$S \cap T$ は空である。実はこれは常に成り立つ。

$$(4a+3)(4b+3) = 16ab + 12a + 12b + 9 = 4(4ab + 3a + 3b + 2) + 1 \in S.$$

混合した積も後で必要になる。

$$(4a+1)(4b+3) = 16ab + 12a + 4b + 3 = 4(4ab + 3a + b) + 3 \in T.$$

まとめると、T の数を $\equiv -1 \pmod 4$ と書けば、奇数の積は $\equiv (-1)^k \pmod 4$ となる。ここで k は T からの因数の個数である。したがって、k が偶数ならば積は S に属し、k が奇数ならば T に属する。

小問 (iii)

$n \in T$ を合成数（composite）とし、$n = p_1 p_2 \cdots p_r$ と素数の積に表す。n は奇数であるから、各 p_i も奇数であり、小問 (i) より各 p_i は S または T に属する。

背理法（proof by contradiction）により、すべての p_i が S に属すると仮定する。小問 (ii) をくり返し用いると、$p_1 p_2 \in S$、次に $(p_1 p_2) p_3 \in S$、以下同様にして $n \in S$ となる。しかし $n \in T$ かつ $S \cap T = \varnothing$ であるから、これは矛盾である。よって、n の素因数の少なくとも一つは T に属する。（偶奇の言葉でいえば、$n \equiv -1$ となるには $\equiv -1$ である因数が奇数個、したがって少なくとも一個必要である。）

小問 (iv)(a)

まず $1 \notin T$ であるから、T の元はすべて 3 以上であることに注意する。

すべての $n \in T$ は、T-素数であるか、T-素数の積である。 n についての強い帰納法（strong induction）を用いる。n が T-素数ならば示すことはない。そうでなければ、$k \geq 2$ かつ各 $t_i \in T$ として $n = t_1 t_2 \cdots t_k$ と書ける。各 $t_i \geq 3$ であるから各 $t_i \leq n/3 < n$ であり、帰納法の仮定により各 t_i は T-素数であるか T-素数の積である。これらを $n = t_1 \cdots t_k$ に代入すれば、n は T-素数の積として表される。

> **?** **考えてみよう** T-素数の積は得られたが、なぜその個数は**奇数**でなければならないのか？

T-素数はすべて T に属するので、$\equiv -1 \pmod 4$ である。したがって、小問 (ii) の最後に述べた規則により、それらを m 個掛けた積は $\equiv (-1)^m \pmod 4$ となる。もし m が偶数ならば、積は $\equiv 1$ となり、T ではなく S に属することになる。積は $n \in T$ であるから、m は奇数である。よって、すべての $n \in T$ は T-素数であるか、奇数個の T-素数の積であり、これが示すべきことであった。

T-素数が素数であるとは限らないことに注意しよう。$15 = 3 \times 5$ は T-素数である。なぜなら $5 \notin T$ であり、1 より大きい数への分解は 3×5 しかないからである。

小問 (iv)(b)

15 についての注意と同じ考え方が S でも使える。T に属する二つの素数の積は S に属するが、S の中では分解できない。そこで

$$9 = 3 \times 3, \qquad 21 = 3 \times 7, \qquad 49 = 7 \times 7.$$

をとる。いずれも S に属する。また、いずれも S-素数である。実際、1 と自分自身以外の約数は 3 または 7 であり、これらは S ではなく T に属する。(21 の約数は $1, 3, 7, 21$ である。) ここで

$$441 = 9 \times 49 = 21 \times 21,$$

であり、$441 = 4 \times 110 + 1 \in S$ である。これらは 441 の S-素数への本当に異なる二つの分解である。一つ目は 9 と 49 を用い、二つ目は 21 を二回用いている。よって 441 が求める例である。

考えてみよう この例はどのようにすれば見つけられただろうか？

通常の整数では $441 = 3^2 \times 7^2$ であり、素数 $3, 7$ は T に属する。S の中では 3 や 7 を一つだけ切り離すことはできないので、T-素数は二つずつ組にしなければならない。3 が二つ、7 が二つあれば、組の作り方は $(3 \cdot 3)(7 \cdot 7)$ と $(3 \cdot 7)(3 \cdot 7)$ の二通りある。相異なる素数 $p, q \in T$ による任意の p^2q^2 でも同様にうまくいく。たとえば $9 \times 121 = 33 \times 33$ である。

検算

- 小さい場合を試す：$5 \times 9 = 45 \in S$、$3 \times 7 = 21 \in S$、$5 \times 7 = 35 \in T$。
- (iii) について：$15 = 3 \times 5$ と $35 = 5 \times 7$ は T に属し、いずれも T に属する素因数 (3、7) をもつ。
- コンピュータで調べると、3000 未満のすべての $n \in T$ について、T-素数へのどの分解も因数の個数は奇数である。T-素数は $3, 7, 11, 15, 19, 23, 31, 35, \ldots$ と始まる。$27 = 3 \times 3 \times 3$ は T-素数ではないことに注意しよう。因数は三個で、奇数である。

よくある間違い

- 具体例を確かめずに、T の二つの元の積は T に属すると主張してしまう。$3 \times 3 = 9$ を見ればすぐに決着がつく。

- X-素数が素数であるとは限らないことを忘れる。これこそが (iv)(b) の要点である。9 と 21 は S-素数である。
- (iv)(a) で、因数の個数が奇数であることだけを証明し、そもそも T-素数への分解が存在することを示し忘れる。

STEP のその先へ

集合 S は乗法について閉じている（closed under multiplication）が、その「素数」による分解は一意的ではない。これは（ヒルベルト数（Hilbert numbers）と呼ばれることもある）古典的な簡単なモデルであり、$\mathbb{Z}[\sqrt{-5}]$ のような環（ring）で何がうまくいかなくなるかを示している。そこでは $6 = 2 \times 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ となる。このような環で分解の一意性を回復しようとする試みから、イデアル（ideal）と代数的整数論（algebraic number theory）が生まれた。Davenport の *The Higher Arithmetic*（『高等算術』）は、$\mathbb{Z}$ における素因数分解の一意性がなぜ証明を要する定理なのかを説明しており、Allenby の *Rings, Fields and Groups*（『環・体・群』）は、それが成り立たない環を扱っている。

Beyond STEP 解答集：https://beyondstep.keithmcnulty.org/ja/。解答本文は CC0 1.0 である。問題そのものは © Cambridge University Press & Assessment に帰属し、ここには掲載していない。英語版から機械翻訳したものであり、まだ校閲を経ていない。